

## CLAIMS

- 1 1. Apparatus for tightly-coupling hardware data encryption functions with software-  
2 based protocol decode processing within a pipelined processor/of a programmable proc-  
3 essing engine in a network switch, the apparatus comprising:  
4 an encryption execution unit contained within the pipelined processor; and  
5 a software and hardware interface that enables the encryption execution unit to  
6 efficiently cooperate with resources of the pipelined processor.
- 1 2. The apparatus of Claim 1 wherein the encryption execution unit is an encryption  
2 tightly coupled state machine (TCSM) unit that is selectively invoked within the pipe-  
3 lined processor.
- 1 3. The apparatus of Claim 2 wherein a software portion of the interface comprises native  
2 encryption opcodes provided within an instruction set of the pipelined processor to enable  
3 selective access to the encryption TCSM unit.
- 1 4. The apparatus of Claim 3 wherein the resources include a plurality of busses internal  
2 to the pipelined processor and wherein a hardware portion of the interface allows the en-  
3 cryption TCSM unit to utilize the internal buses in response to decode processing of the  
4 native encryption opcodes.
- 1 5. The apparatus of Claim 4 wherein the pipelined processor is microcontroller core  
2 (TMC) processor having a multi-stage pipeline architecture that includes an instruction  
3 fetch stage, an instruction decode stage, an execution stage and a memory write-back  
4 stage.

- 1 6. The apparatus of Claim 5 wherein the TMC processor further includes an arithmetic  
2 logic unit, at least one internal register, an instruction fetch and decode unit and the en-  
3 cryption TCSM unit organized as a data path.
- 1 7. The apparatus of Claim 5 wherein the encryption TCSM unit comprises a data en-  
2 cryption standard (DES) functional component cooperatively coupled to a sub-key gen-  
3 eration functional component.
- 1 8. The apparatus of Claim 7 wherein the DES functional component comprises state ma-  
2 chine hardware used to execute each round of a DES function.
- 1 9. The apparatus of Claim 7 wherein the sub-key generation functional component com-  
2 prises state machine hardware that generates a sub-key as needed for each round of the  
3 DES function.
- 1 ~~10. A method for tightly-coupling hardware data encryption functions with software-~~  
2 ~~based protocol decode processing within a pipelined processor of a programmable proc-~~  
3 ~~essing engine in a network switch, the method comprising the steps of:~~  
4 ~~providing an encryption execution unit within the pipelined processor; and~~  
5 ~~selectively accessing the encryption execution unit through an integrated hard-~~  
6 ~~ware and software interface of the pipelined processor that allows efficient cooperation~~  
7 ~~between the encryption execution unit and resources of the pipelined processor.~~
- 1 11. The method of Claim 10 wherein the integrated interface comprises native encryption  
2 opcodes contained within an instruction set of the pipelined processor and wherein the  
3 step of selectively accessing comprises the step of issuing the native encryption opcodes  
4 directly to the encryption execution unit to substantially reduce encryption setup latency.

1 12. The method of Claim 11 further comprising the steps of, wherein the pipelined proc-  
2 essor is a microcontroller core (TMC) processor having a multi-stage pipeline architec-  
3 ture that includes an instruction decode stage and an execution stage:

4        decoding the native encryption opcodes at the instruction decode stage; and  
5        in response to the step of decoding, invoking the encryption execution unit to per-  
6 form encryption/decryption functions at the execution stage.

1 13. The method of Claim 12 further comprising the steps of, wherein the encryp-  
2 tion/decryption functions are performed on plaintext stored at the network switch:

3        protocol processing of protocols contained in the plaintext to determine an appro-  
4 priate encryption algorithm;

5        upon determining the appropriate encryption algorithm, immediately starting an  
6 operation to fetch initial keys needed to perform the encryption/decryption functions; and

7        upon fetching the keys, providing the keys to the encryption execution unit within  
8 the TMC processor.

1 14. The method of Claim 13 wherein the resources include a plurality of high-  
2 performance busses internal to the TMC processor, and wherein the step of invoking  
3 comprises the step of:

4        accessing the internal busses through the integrated interface to simultaneously  
5 load an encryption key and store a previous encryption result.

1 15. The method of Claim 12 further comprising the step of, wherein the the encryption  
2 execution unit is an encryption tightly coupled state machine (TCSM) unit:

3        initializing the encryption TCSM unit in response to execution of a first instruc-  
4 tion that defines the form of operation to be performed.

1 16. The method of Claim 15 wherein the encryption TCSM unit comprises a data en-  
 2 cryption standard (DES) functional component cooperatively coupled to a sub-key gen-  
 3 eration functional component and wherein the step of initializing comprises the steps of:  
 4 decoding a first portion of the first instruction to initialize the DES functional  
 5 component; and  
 6 decoding a second portion of the first instruction to initialize the sub-key genera-  
 7 tion functional component.

1 17. The method of Claim 16 further comprising the step of:  
 2 executing a second instruction having a micro-opcode field containing a native  
 3 encryption opcode that specifies loading an initial key from a memory into the sub-key  
 4 generation functional component of the encryption TCSM unit.

1 18. The method of Claim 17 further comprising the step of:  
 2 performing a DES function on the plaintext in response to execution of a third in-  
 3 struction having a micro-opcode field containing a native encryption code that specifies  
 4 loading of the plaintext into the DES functional component of the encryption TCSM unit  
 5 and initiating DES operations; and  
 6 upon completing the DES operations, storing ciphertext results in an internal reg-  
 7 ister coupled to the DES functional component.

1 19. The method of Claim 18 further comprising the step of:  
 2 executing a fourth instruction to store the ciphertext results contained in the inter-  
 3 nal register to a location in the memory.

1 20. A programmable processing engine of a network switch comprising:  
 2 an input header buffer;  
 3 an output header buffer; and

B3  
CONF

4 a plurality of processing complex elements symmetrically arrayed into rows and  
5 columns that are embedded between the input header buffer and an output header buffer,  
6 each processing complex element comprising a microcontroller core having an encryption  
7 tightly coupled state machine (TCSM) unit that is selectively invoked through an inte-  
8 grated hardware and software interface of the microcontroller core to allow efficient co-  
9 operation between the encryption TCSM unit and data path resources of the microcontrol-  
10 ler core.

Add  
C16 at